# BACKGROUND INVESTIGATIONS AND SECURITY CLEARANCES

## 1. PURPOSE

This Directive establishes policy and guidance for protecting Animal Plant and Health Inspection Service (APHIS) computing systems, Local Area Networks (LANs), and Wide Area Networks (WANs) by identifying the risk and sensitivity levels of Information Technology (IT) positions and corresponding requirements for background investigations and security clearances as applicable. This policy is intended to protect government computers, data, networks, and resources from being accessed by people who have risky or unfavorable backgrounds.

## 2. SCOPE

This Directive affects all employees, contractors, and State agency employees using the APHIS LAN/WAN/voice networks. It does not affect members of the public accessing APHIS data.

## 3. AUTHORITIES/REFERENCES

Federal regulations regarding personnel security requirements can be found in 5 CFR 731, 732, and 736 (revised January 2001).

a. Section 731.106: Designation of public trust positions and investigative requirements.

(1) **Risk Designation**. Agency heads will designate every competitive service position within the agency at a high, moderate, or low risk level as determined by the position's potential for adverse impact to the efficiency and integrity of the service.

(2) **Public Trust Positions**. Positions at the high or moderate risk levels would normally be designated as "Public Trust" positions. Such positions may involve policy making, major program responsibility, public safety and health, law enforcement duties, fiduciary responsibilities, or other duties demanding a significant degree of public trust; and positions involving access to, or operation or control of, financial records, with a significant risk for causing damage or realizing personal gain.

(3) Minimal investigative requirements correlating to risk levels will be established in supplemental guidance provided by the Office of Personnel Management (OPM).

b. Section 731.302: Risk designation and investigative requirements.

Suitability reinvestigations: (1) Every incumbent of a competitive service position: "(i) designated High Risk, Moderate Risk and Law enforcement or public safety … shall be subject to a periodic reinvestigation . . . 5 years after placement, and at least once each succeeding 5 years."

c. 5 CFR 732, Section 732.201: Sensitivity level designations and investigative requirements.

For purposes of this part, the head of each agency will designate, or cause to be designated, any position within the department or agency the occupant of which could bring about, by virtue of the nature of the position, a materially adverse effect on national security as a sensitive position at one of three sensitivity levels: Special-Sensitive, Critical-Sensitive, or Noncritical-Sensitive.

## 4. DEFINITIONS

a. **Security clearance.** Formal certification that refers to eligibility for access to National Defense Classified Information.

b. **Public Trust positions.** Positions with the potential for action or inaction by the incumbent to affect the integrity, efficiency, and effectiveness of Government operations.

c. **National security positions.** (1) Positions involving activities of the Government that are concerned with the protection of the nation from foreign aggression or espionage, including development of defense plans or policies, intelligence or counterintelligence activities, and related activities concerned with the preservation of the military strength of the United States; and (2) positions that require regular use of, or access to, classified information. (Most of APHIS's positions will not fall under National Security positions, but there will be a few.) Sensitivity level designations are based upon an assessment of the degree of damage that an individual could cause to the National Security. Below lists the three types of sensitivity levels for National Security positions.

(1) **Critical-sensitive.** High risk positions that require any national security clearance and have the potential for exceptionally grave damage to national security. Exceptionally grave damage equates to Department of Defense top secret information.

(2) **Noncritical-sensitive.** Positions that have potential for moderate to serious damage to national security. Serious damage equates to Department of Defense secret information.

(3) **Non-sensitive.** Positions that have potential for limited damage to the national security. Damage equates to Department of Defense confidential information.

d. **Need-to-know.** A principle by which information is provided only to those with a legitimate need for that information.

e. **Sensitive information.** Any information (including the loss, misuse, or unauthorized access to, or modification of) which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a, Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. (Public Law 100-235, Computer Security Act of 1987.)

f. **High risk.** Potential for exceptionally serious impact on an agency or program mission or the overall efficiency of the service. (Background Investigation (**BI**))

g. **Moderate risk.** Potential for moderate to serious impact on an agency or program mission or efficiency of the service. (Minimum Background Investigation (**MBI**))

h. **Low risk.** Potential for limited impact on an agency or program mission or efficiency of the service. (National Agency Check Investigation (**NACI**))

## 5. BACKGROUND

The Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, requires that agencies "… screen individuals who are authorized to bypass significant technical and operational security controls of the system commensurate with the risk and magnitude of harm they could cause."

In addition, USDA Office of Cyber Security's call for yearly security plans (April 10, 2001) states: "… anyone handling sensitive or departmental priority applications or systems must have a background check. Systems administrators, network administrators, field security officers, and others in the agency who have the potential or position to adversely affect security of agency information must have a background check…" and possibly a secret level of access, if the position involves access to classified information. These requirements apply to all contractors for IT programs or services and should be written into the initial requirements for these contracts.

## 6. POLICY

It is APHIS policy that:

a. Federal, State, and county employees; contractors; and non-Federal employees using APHIS LAN/WAN/voice networks will have the following background investigations/security clearances performed. See Table 1 for clarification of what background investigation/security clearance each employee needs.

(1) National Agency Check with Local Agency Check (NAC/LAC).

(2) Limited Background Investigation (LBI).

(3) MBI.

(4) BI or Single-Scope Background Investigation (SSBI).

(5) Secret Level or have existing clearance validated or passed at the needed level.

b. Background investigations must be conducted on employees commensurate with their position risk and/or sensitivity, level of access, and need to know. Anyone handling sensitive or departmental priority applications or systems must have a background investigation. At the minimum, all employees will be subject to an NACLC. Employees include both permanent and temporary APHIS employees, contractors, and State agency personnel accessing the APHIS LAN/WAN/Voice Networks with the privileges that would be afforded an APHIS employee performing in the same position.

c. The requirement for security clearances for IT employees is based on an assessment of position sensitivity, criticality, and ability to do grave harm. Where separation of duties is weak, security clearance requirements must be more stringent. All Information Systems Security Program Managers (ISSPMs) and their Deputies must obtain top secret clearances so that they can attend threat briefings conducted at the confidential, secret, or top secret level by Government agencies such as the Federal Bureau of Investigation, the National Security Agency, the Department of Homeland Security, etc. Systems administrators, network administrators, database administrators, and others in the Agency who have the potential or position to adversely affect security of Agency information must have a background investigation and receive a favorable determination at the secret level of access. These requirements apply to both Government employees and permanent contractor employees. The ISSPM and Deputy for APHIS, working directly with the Human Resources Division (HRD) specialist, are responsible for ensuring that IT security personnel have the necessary security clearances.

d. When a higher level of access is needed to meet operational or contractual exigencies and: 1) is not expected to be of a recurring nature; 2) will not exceed 180 days; and 3) is limited to specific, identifiable information, temporary access may be granted by security personnel authorized by the Agency.

e. Individuals, whose jobs, scope of responsibilities, levels of access, and/or duties significantly change, so that their initial investigation is insufficient to support the incumbents' current needs, require an updated, upgraded reinvestigation within 120 days of reassignment, promotion, or reclassification.

f. A periodic reinvestigation, dependent on the original level of investigation or clearance, is required and will be coordinated by HRD. See Table 1 for security clearance reinvestigation intervals for various employee categories.

g. All accesses will be contingent on favorable investigations or periodic reinvestigations. Individuals who occupy positions that require favorable background investigations, and whose investigations are returned unfavorable, will have all accesses suspended or revoked until such time that the individual can address the deficiencies and successfully undergo a favorable investigation. In the case of individuals who need "secret" clearance and fail, they must be denied access to the computers with sensitive or confidential data until the situation is resolved. In the case of individuals who fail a BI or LBI, the system administrator rights associated with the login ID and the appropriate user IDs on any servers must be disabled until the situation is resolved.

   All job vacancies for these specific job categories must include the agreement that hiring is based on the assumption the selected candidate will pass the required background check. Failure to do so will result in the employee being removed from this position immediately.

h. As noted throughout this Directive, permanent contractors must adhere to the same clearance levels and reinvestigation requirements as Federal employees. The ISSPM must review permanent contractor clearances to ensure the clearance is adequate and current. Contracting officials are responsible for making sure all current and future contracts include official language addressing security clearances.

i. The General Services Administration (GSA), Office of Federal Protective Services (FPS), is responsible for background checks for cleaning and cafeteria employees in major Government complexes.

j. Classified national security information will be handled and secured in accordance with Department Manual 3440-1. All violations and sanctions are applicable.

Table 1. Background Investigation/Security Clearance Levels

| Employees | Security Clearance Level | Required Security Clearance Form | Frequency |
|---|---|---|---|
| All Federal employees (non-IT) | NAC/LAC | **SF-85, OF-306, OF-612, and SF-87 Fingerprint Chart** | Every 10 years |
| All Federal employees (including IT employees not listed below) | NAC/LAC | **SF-85, OF-306, OF-612, and SF-87 Fingerprint Chart** | Every 10 years |
| Information Systems Security Program Managers (ISSPMs), Deputy ISSPMs | SSBI with Top Secret Level of Access | **SF-86, Fair Credit Form OF-306, OF-612, and SF-87 Fingerprint Chart** | Every 5 years |
| System Administrators, Network Administrators, Database Administrators, Customer Service Representatives, and Program (ISSMs & ISSOs) | BI with Secret Level of Access | **SF-86, Fair Credit Form, OF-306, OF-612, and SF-87 Fingerprint Chart** | Every 5 years |
| Supervisory System Administrators or Network Administrators | BI with Secret Level of Access | **SF-86, Fair Credit Form, OF-306, OF-612, and SF-87 Fingerprint Chart** | Every 5 years |
| CIO, TRM Manger, CS Manager, and FPS Manager | SSBI with Top Secret Level of Access | **SF-86, Fair Credit Form, OF-306, OF-612, and SF-87 Fingerprint Chart** | Every 5 years |
| Application Programmers | BI with Secret Access | **SF-86, Fair Credit Form, OF-306, OF-612, and SF-87 Fingerprint Chart** | Every 5 years |
| Technical Help Desk Employees | BI with Secret Access | **SF-86, Fair Credit Form, OF-306, OF-612, and SF-87 Fingerprint Chart** | Every 5 years |
| Program Help Desk Employees | NAC/LAC | **SF-85, OF-306, OF 612, and SF-87 Fingerprint Chart** | Every 10 years |
| Financial Employees | NAC/LAC | **SF-85, OF-306, OF-612, and SF-87 Fingerprint Chart** | Every 10 years |
| Human Resources Staff | NAC/LAC | **SF-85, OF-306, OF-612, and SF-87 Fingerprint Chart** | Every 5 years |
| Contracting Officers | NAC/LAC | **SF-85, OF-306, OF-612, and SF-87 Fingerprint Chart** | Every 5 years |
| Non-Federal Employees | NAC/LAC | **SF-85, OF-306, OF-612, and SF-87 Fingerprint Chart** | Every 10 years |

**Notes:**

- If access to classified information is required for any IT position, a higher level of investigation may be required. An SSBI is required if access to Top Secret and/or Sensitive Compartment Information is required.

- If a person who has a security clearance moves to another job assignment that does not require or requires a lower security clearance, his/her clearance level should be reduced accordingly.

- Contractors permanently assigned to IT restricted space, as defined in OCIO-Cyber Security Policy 005, will have an MBI prior to working in the facility.

- Clearance does not automatically give you access to classified information; there must be a "need-to-know."

## 7. RESPONSIBILITIES

a. The Agency Information Systems Security Program Manager (ISSPM) and his/her Deputies must:

(1) Periodically review and update this Directive as required.

(2) Obtain and maintain a security clearance level of top secret.

(3) Coordinate with the HRD specialists to ensure that IT security employees have the necessary security clearances and that periodic reviews are performed.

(4) Review permanent contractor clearances to ensure the clearance is adequate and current. Submit information to the USDA Office of Procurement and Property Management staff to have clearance validated for access to Departmental network. Validation must be completed before access is granted.

(5) Distribute this Directive to all employees, contractors, and other county-based agency partners, and check that distribution has occurred to all levels of the organization.

b. Program Managers and IT Supervisors must:

(1) Identify positions managed by them which require a security clearance.

(2) Ensure staff members covered under this Directive have received the

proper security clearance and initial an annual security training.

(3) Coordinate with an HRD specialist to include security clearance requirements as a part of vacancy announcements.

(4) Ensure that security clearance levels remain sufficient as the scope of responsibilities and levels of access are modified for employees.

c. Contracting officials must ensure all current and future contracts include official language addressing both initial and periodic-reinvestigation security clearances.

d. HRD Specialists must:

(1) Initiate security clearance investigations for new employees.

(2) Coordinate periodic reinvestigations, dependent on the original level of investigation or clearance.

(3) Coordinate with program managers and IT supervisors to ensure all applicable staff has received the necessary security clearances.

(4) Coordinate with building and contract officials to ensure appropriate checks have been performed for cleaning and cafeteria employees not covered by the GSA, FPS.

## 8. INQUIRIES

a. Direct inquiries or requests for changes to this Directive to: ITD, FPS, Riverdale, MD 20737, or call (301) 734-5084.

b. Copies of current APHIS directives can be accessed on the Internet at www.aphis.usda.gov/library.

/s/
Michael C. Gregoire
Chief Information Officer